UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,391	10/07/2003	Jong-Su Lim	44824	5463

7590 11/28/2006

Peter L. Kendall
Roylance, Abrams, Berdo & Goodman, L.L.P.
Suite 600
1300 19th Street, N.W.
Washington, DC 20036

EXAMINER	
DEBNATH, SUMAN	

ART UNIT	PAPER NUMBER
2196	

DATE MAILED: 11/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/679,391	LIM, JONG-SU	
	Examiner	Art Unit	
	Suman Debnath	2196	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10/07/03* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-12 are pending in this application.

Drawings

2. Figures 1, 2A, 2B, 3 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to because of the following informalities:

Reference character "516" is used in specification (page 12, line 26) but "360" is used in FIG. 5 to designate "FI.sub.2,3".

Reference character "515" is used to designate "FL.sub 2,2" in specification (page 12, line 21) but "FI.sub.2,2" in FIG. 5.

Reference character "360" is used in FIG. 3 to designate "ZE2 unit" but "FI.sub.2,3" in FIG. 5.

Reference character "360" is used to receive the signal "RR.sub.1" in specification (page 6, line 5) but "360" is used to receive the signal "RR.sub.2" in FIG. 3.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

4. The disclosure is objected to because of the following informalities:

Reference character "360" is used in specification to receive the signal "RR.sub.1" (page 6, line 5) but "RR.sub.2" in FIG. 3.

Specification discloses, "S71 operator 740 generates a **7-but signal y0, y1, ..., y6**" (page 14, lines 11-12) and "S71 operator 740 generates the **9-bit signal y1, y2, ...,**

y6" (page 14, lines 17-20). Applicant shows inconsistency of generating signal by the same unit in the above discloser.

Appropriate correction is required.

Claim Objections

5. Claim 1 is objected to because of the following informalities:

Claim 1 recites the limitations "the second ciphertext bit stream" in line 9 and "the first ciphertext bit stream" in line 10. There is insufficient antecedent basis for these limitations in the claim.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 3 recites the limitation "first predetermined encryption codes" in line 1. It is unclear whether this is intended to be the same as or different from the "first predetermined encryption codes" recited in claim 2. Examiner will treat the limitation of claim 3 as "second predetermined encryption codes" for the purpose of examination as the subscript of KO and KI refers to 2,1; 2,2; 2,3.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-5 and 7-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's admitted prior art, hereinafter "AAPA," in view of 3rd Generation Partnership Project, "Document 2: KASUMI Specification" Release 4, 2001-08-28, hereinafter "DKS".

10. As to claim 1, AAPA discloses an encryption method for dividing a first plaintext bit stream of length 2n into first and second sub-bit streams of length n (FIG. 1, item 210, L.sub.01 is an input to FO1 unit which takes two sub-bit stream input, see FIG. 2B), dividing a second plaintext bit stream of length 2n into third and fourth sub-bit streams of length n (FIG. 1, item 220, input of FO2 takes two sub-bit stream), and generating a ciphertext bit stream of length 2n from the first, second, third and fourth sub-bit streams using 2-rounds of encryption (FIG. 1, item 210 and 220 provides 2-rounds of encryption), the method comprising the steps of:

Performing a first-round of encryption by outputting the second ciphertext bit stream being output with a predetermined time delay from the first ciphertext bit stream after receiving the first and second sub-bit streams and generating first ciphertext bit streams of length n by encrypting the first and second sub-bit streams with predetermined first encryption codes (FIG. 2B, specification, page 3, lines 23-30 and page 4, lines 1-15; AAPA discloses a block diagram of FOi units which generates first and second ciphertext bit streams R.sub.4' and L.sub.4' after receiving the first sub-bit stream L.sub.0' and second sub-bit stream R.sub.0' with predetermined first encryption codes KO.sub.1,1, KO.sub.1,2, KO.sub.1,3, KI.sub.1,1, KI.sub.1,2, and KI.sub.1,3; Second ciphertext bit stream L.sub.4' being output with predetermined time delay, see e.g., FIG. 2B, item 50.).

Generating a first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first ciphertext bit stream and the third sub-bit stream (specification, page 2, lines 14-17, FIG. 1, which teaches output of FO1 unit performs an exclusive-OR operation with R.sub.0 to provide input for second FO2 unit); generating a second operated ciphertext bit stream by performing a logical exclusive-OR operation on the second ciphertext bit stream and the fourth sub-bit stream (specification, page 2, lines 14-17, FIG. 1, , which teaches output of FO1 unit performs an exclusive-OR operation with R.sub.0 to provide input for second FO2 unit).

Performing a second-round encryption by outputting the third and fourth ciphertext bit streams (specification, page 2, lines 8-10, describes FOi units. "i" reads on second round, see e.g., FIG. 1, item 220 and FIG. 2B teaches the implementation of

item 220, R.sub.4' reads on outputting the third ciphertext bit and L.sub.4' reads on outputting fourth ciphertext bit stream) after receiving the first operated ciphertext bit stream and the second operated ciphertext bit stream having the predetermined time delay (FIG. 2B, L.sub.0' reads on first operated ciphertext bit stream and R.sub.0' reads on second operated ciphertext bit stream; FIG. 1 teaches second round (item 220) that takes input from output of first round (item 210) combined with R.sub.0 by performing an exclusive-OR operation which causes time delay) and generating third and fourth ciphertext bit streams of length n by encrypting the first operated ciphertext bit stream and the second operated ciphertext bit stream with predetermined encryption codes (FIG. 2B, specification, page 3, lines 23-30 and page 4, lines 1-15).

AAPA doesn't explicitly disclose performing the corresponding second-round encryption using predetermined second encryption codes. However, using second set of predetermined encryption code for second round encryption is standard in Kasumi encryption algorithm as taught by DKS (page 12, section 4.3, which describes KO.sub.i=KO.sub.i,1 || KO.sub.i,2 || KO.sub.i,3 and KI.sub.i= KI.sub.i,1 || KI.sub.i,2, || KI.sub.i,3; "i" represents rounds, see e.g., page 10, section 2.3, line 10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify AAPA by using second set of predetermined encryption code for second round encryption as taught by DKS in order to increase the confidentiality and integrity of the encrypted data. Furthermore, one would be motivated to do so to transmit data over the public network.

11. As to claim 2, AAPA discloses the first predetermined encryption codes comprises at least one of KO.sub.1,1, KO.sub.1,2, KO.sub.1,3, KI.sub.1,1, KI.sub.1,2, and KI.sub.1,3 (specification, page 2, lines 26-30 and page 3, lines 2-11).

12. As to claim 3, DKS discloses the second predetermined encryption codes comprises at least one of KO.sub.2,1, KO.sub.2,2, KO.sub.2,3, KI.sub.2,1, KI.sub.2,2, and KI.sub.2,3 (specification, page 12, section 4.3, which describes KO.sub.i=KO.sub.i,1 || KO.sub.i,2 || KO.sub.i,3 and KI.sub.i= KI.sub.i,1 || KI.sub.i,2, || KI.sub.i,3, "i" reads on 2, see e.g., page 10, section 2.3, line 10).

13. As to claim 4, AAPA discloses the first-round encryption (FIG. 1, item 210) step comprises the steps of: generating a first signal by performing a logical exclusive-OR operation on the first sub-bit stream and the first encryption code KO.sub.1,1 to provide a first exclusive-OR operated bitstream (specification, page 3, lines 26-29), encrypting the first exclusive-OR-operated bit stream with the first encryption code KI.sub.1,1 to provide a first encrypted signal (specification, page 3, lines 29-30), and performing a logical exclusive-OR operation on the first encrypted signal and the second sub-bit stream (specification, page 4, lines 2-3); delayed by time required for the encryption (specification, page 4, line 1); generating the first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second sub-bit stream and the first

encryption code KO.sub.1,2 (specification, page 4, lines 3-5), to provide a second exclusive-OR operated bitstream encrypting the second exclusive-OR-operated bit stream with the first encryption code KI.sub.1,2, to provide a second encrypted signal (specification, page 4, lines 5-6); and performing a logical exclusive-OR-operation on the second encrypted signal and the first signal (specification, page 4, lines 7-8); generating the second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first signal and the first encryption code KO.sub.1,3 to provide a third exclusive-OR operated bitstream (specification, page 4, lines 8-10); encrypting the third exclusive-OR-operated bit stream with the first encryption code KI.sub.1,3 (specification, page 4, lines 10-11); and performing a logical exclusive-OR-operation on the encrypted signal with the first sub-bit stream delayed by time required for the encryption (specification, page 4, lines 11-14).

14. As to claim 5, AAPA discloses the second-round encryption (FIG. 1, item 220) step comprises the steps of: generating a second signal by performing a logical exclusive-OR-operation the first operated ciphertext bit stream and the encryption code to provide a fourth exclusive-OR operated bitstream (specification, page 3, lines 26-29); encrypting the fourth exclusive-OR-operated bit stream with the encryption code to provide a third encrypted signal (specification, page 3, lines 29-30); performing a logical exclusive-OR-operation on the third encrypted signal and the second operated ciphertext bit stream to provide a fifth exclusive-OR operated bitstream (specification, page 4, lines 2-3); generating the third ciphertext bit stream by performing a logical

exclusive-OR-operation on the second operated ciphertext bit stream and the encryption code (specification, page 4, lines 3-5); encrypting the fifth exclusive-OR-operated bit stream with the encryption code to provide a fourth encrypted signal (specification, page 4, line 5-8); and performing a logical exclusive-OR-operation on the fifth encrypted signal and the second signal (specification, page 4, lines 9-10); delayed by time required for the encryption (specification, page 4, line 12); and generating the fourth ciphertext bit stream by performing a logical exclusive-OR-operation on the second signal and the encryption code (specification, page 4, lines 7-10); encrypting the sixth exclusive-OR-operated bit stream with the encryption code (specification, page 4, lines 10-11); and performing a logical exclusive-OR-operation on the encrypted signal with the third ciphertext bit stream (specification, page 4, lines 11-14).

AAPA doesn't explicitly disclose performing the corresponding second-round encryption using predetermined second encryption codes KO.sub.2,1, KI.sub.2,1, KO.sub.2,2, KI.sub.2,2, KO.sub.2,3 and KI.sub.2,3. However, using second set of predetermined encryption code for second round encryption is standard in Kasumi encryption algorithm as taught by DKS (page 12, section 4.3, which describes KO.sub.i=KO.sub.i,1 || KO.sub.i,2 || KO.sub.i,3 and KI.sub.i= KI.sub.i,1 || KI.sub.i,2, || KI.sub.i,3, "i" reads on 2, see e.g., page 10, section 2.3, line 10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify AAPA by using second set of predetermined encryption code for second round encryption as taught by DKS in order to increase the

confidentiality and integrity of the encrypted data. Furthermore, one would be motivated to do so to transmit data over the public network.

15. As to claim 7, AAPA discloses the encryption method wherein a 16-bit input bit stream is divided into a 9-bit stream and a 7-bit stream (specification, page 4, lines 22-24, FIG. 3), a 9-bit ciphertext bit stream is generated from the 9-bit stream using a first equation (specification, page 4, lines 24-25), and a 7-bit ciphertext bit stream is generated from the 7-bit stream using a second equation in each of the sub-encryptions (speciation, page 5, line 12), wherein said first equation comprises y 0 = (x0x2) ⊕ x3 ⊕ (x2x5) ⊕ (x5x6) ⊕ (x0x7) ⊕ (x1x7) ⊕ (x2x7) ⊕ (x4x8) ⊕ (x5x8) ⊕ (x7x8) ' ⊕1 ' ; y 1 = x1 ⊕ (x0x1) ⊕ (x2x3) ⊕ (x0x4) ⊕ (x1x4) ⊕ (x0x5) ⊕ (x3x5) ⊕ x6 ⊕ (x1x7) ⊕ (x2x7) ⊕ (x5x8) ' ⊕1 ' ; y2 = x1 ⊕ (x0x3) ⊕ (x3x4) ⊕ (x0x5) ⊕ (x2x6) ⊕ (x3x6) ⊕ (x5x6) ⊕ (x4x7) ⊕ (x5x7) ⊕ (x6x7) ⊕ x8 ⊕ (x0x8) ' ⊕ 1 ' ; y3 = x0 ⊕ (x1x2) ⊕ (x0x3) ⊕ (x2x4) ⊕x5 ⊕ (x0x6) ⊕ (x1x6) ⊕ (x4x7) ⊕ (x0x8) ⊕ (x1x8) ⊕ (x7x8) ; y4 = (x0x1) ⊕ (x1x3) ⊕x4 ⊕ (x0x5) ⊕ (x3x6) ⊕ (x0x7) ⊕ (x6x7) ⊕ (x1x8) ⊕ (x2x8) ⊕ (x3x8) ; y5 = x2 ⊕ (x1x4) ⊕ (x4x5) ⊕ (x0x6) ⊕ (x1x6) ⊕ (x3x7) ⊕ (x4x7) ⊕ (x6x7) ⊕ (x5x8) ⊕ (x6x8) ⊕ (x7x8) ' ⊕1 ' ; y6 = x0 ⊕ (x2x3) ⊕ (x1x5) ⊕ (x2x5) ⊕ (x4x5) ⊕ (x3x6) ⊕ (x4x6) ⊕ (x5x6) ⊕x7 ⊕ (x1x8) ⊕ (x3x8) ⊕ (x5x8) ⊕ (x7x8) ; y7 = (x0x1) ⊕ (x0x2) ⊕ (x1x2) ⊕ x3 ⊕ (x0x3) ⊕ (x2x3) ⊕ (x4x5) ⊕ (x2x6) ⊕ (x3x6) ⊕ (x2x7) ⊕ (x5x7) ⊕x8 ' ⊕1 ' ; y8 = (x0x1) ⊕x2 ⊕ (x1x2) ⊕ (

x3x4) ⊕ (x1x5) ⊕ (x2x5) ⊕ (x1x6) ⊕ (x4x6) ⊕ x7 ⊕ (x2x8) ⊕ (x3x8)

(specification, page 5, line 1, equation 1);

Second equation comprises y 0 = (x1x3) ⊕ x4 ⊕ (x0x1x4) ⊕ x5 ⊕ (x2x5) ⊕ (x3x4x5) ⊕ x6 ⊕ (x0x6) ⊕ (x1x6) ⊕ (x3x6) ⊕ (x2x4x6) ⊕ (x1x5x6) ⊕ (x4x5x6) ; y 1 = (x0x1) ⊕ (x0x4) ⊕ (x2x4) ⊕ x5 ⊕ (x1x2x5) ⊕ (x0x3x5) ⊕ x6 ⊕ (x0x2x6) ⊕ (x3x6) ⊕ (x4x5x6) ' ⊕ 1 ' ; y2 = x0 ⊕ (x0x3) ⊕ (x2x3) ⊕ (x1x2x4) ⊕ (x0x3x4) ⊕ (x1x5) ⊕ (x0x2x5) ⊕ (x0x6) ⊕ (x0x1x6) ⊕ (x2x6) ⊕ (x4x6) ' ⊕ 1 ' ; y3 = x1 ⊕ (x0x1x2) ⊕ (x1x4) ⊕ (x3x4) ⊕ (x0x5) ⊕ (x0x1x5) ⊕ (x2x3x5) ⊕ (x1x4x5) ⊕ (x2x6) ⊕ (x1x3x6) ; y4 = (x0x2) ⊕ x3 ⊕ (x1x3) ⊕ (x1x4) ⊕ (x0x1x4) ⊕ (x2x3x4) ⊕ (x0x5) ⊕ (x1x3x5) ⊕ (x0x4x5) ⊕ (x1x6) ⊕ (x3x6) ⊕ (x0x3x6) ⊕ (x5x6) ' ⊕1 ' ; y5 = x2 ⊕ (x0x2) ⊕ (x0x3) ⊕ (x1x2x3) ⊕ (x0x2x4) ⊕ (x0x5) ⊕ (x2x5) ⊕ (x4x5) ⊕ (x1x6) ⊕ (x1x2x6) ⊕ (x0x3x6) ⊕ (x3x4x6) ⊕ (x2x5x6) ' ⊕1 ' ; y6 = (x1x2) ⊕ (x0x1x3) ⊕ (x0x4) ⊕ (x1x5) ⊕ (x3x5) ⊕ x6 ⊕ (x0x1x6) ⊕ (x2x3x6) ⊕ (x1x4x6) ⊕ (x0x5x6) (specification, page 5, line 15, equation 2) ;

16. As to claim 8, AAPA discloses an encryption apparatus for dividing a first plaintext bit stream of length 2n into first and second sub-bit streams of length n (FIG. 1, item 210, L.sub.01 is an input to FO1 unit which takes two sub-bit stream input, see FIG. 2B), dividing a second plaintext bit stream of length 2n into third and fourth sub-bit streams of length n (FIG. 1, item 220, input of FO2 takes two sub-bit stream), and

generating a ciphertext bit stream of length 2n from the first, second, third and fourth sub-bit streams using 2-rounds of encryption (FIG. 1, item 210 and 220 provides 2-rounds of encryption), the apparatus comprising:

A first ciphering unit (FIG. 1, item 210) for receiving the first and second sub-bit streams (specification, page 3, lines 26-27, L.sub.0' reads on the first sub-bit stream and R.sub.0' reads second sub-bit stream), and generating first and second ciphertext bit streams of length n by encrypting the first and second sub-bit streams with predetermined first encryption codes KO.sub.1,1, KO.sub.1,2, KO.sub.1,3, KI.sub.1,1, KI.sub.1,2, and KI.sub.1,3 the second ciphertext bit stream being output with a predetermined time delay compared to the first ciphertext bit stream (FIG. 2B, specification, page 3, lines 23-30 and page 4, lines 1-15; AAPA discloses a block diagram of FOi units which generates first and second ciphertext bit streams R.sub.4' and L.sub.4' after receiving the first sub-bit stream L.sub.0' and second sub-bit stream R.sub.0' with predetermined first encryption codes KO.sub.1,1, KO.sub.1,2, KO.sub.1,3, KI.sub.1,1, KI.sub.1,2, and KI.sub.1,3; Second ciphertext bit stream L.sub.4' being output with predetermined time delay, see e.g., FIG. 2B, item 50); an operating unit for generating a first operated ciphertext bit stream by performing a logical exclusive-OR-operation on the first ciphertext bit stream and the third sub-bit stream (specification, page 2, lines 14-17, FIG. 1, which teaches output of FO1 unit performs an exclusive-OR operation with R.sub.0 to provide input for second FO2 unit), and generating a second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the second ciphertext bit stream with the fourth sub-bit stream (specification, page 2, lines

14-17, FIG. 1, which teaches output of FO1 unit performs an exclusive-OR operation with R.sub.0 to provide input for second FO2 unit).

A second ciphering unit (FIG. 1, item 220) for receiving the first operated ciphertext bit stream and the second operated ciphertext bit stream having the predetermined time delay (FIG. 2B, L.sub.0' reads on first operated ciphertext bit stream and R.sub.0' reads on second operated ciphertext bit stream; FIG. 1 teaches second round (item 220) that takes input from output of first round (item 210) combined with R.sub.0 by performing an exclusive-OR operation which causes time delay), generating third and fourth ciphertext bit streams of length n by encrypting the first operated ciphertext bit stream and the second operated ciphertext bit stream with predetermined encryption codes (FIG. 2B, specification, page 3, lines 23-30 and page 4, lines 1-15; R.sub.4' reads on the third ciphertext bit and L.sub.4' reads on fourth ciphertext bit stream) and concurrently outputting the third and fourth ciphertext bit streams (specification, page 4, lines 12-15).

AAPA doesn't explicitly disclose the use of second-round encryption using predetermined second encryption codes KO.sub.2,1, KI.sub.2,1, KO.sub.2,2, KI.sub.2,2, KO.sub.2,3 and KI.sub.2,3. However, using second set of predetermined encryption code for second round encryption is standard in Kasumi encryption algorithm as taught by DKS (page 12, section 4.3, which describes KO.sub.i=KO.sub.i,1 || KO.sub.i,2 || KO.sub.i,3 and KI.sub.i= KI.sub.i,1 || KI.sub.i,2, || KI.sub.i,3, "i" reads on 2, see e.g., page 10, section 2.3, line 10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify AAPA by using second set of predetermined encryption code for second round encryption as taught by DKS in order to increase the confidentiality and integrity of the encrypted data. Furthermore, one would be motivated to do so to transmit data over the public network.

17. As to claim 9, AAPA discloses the encryption apparatus wherein the first ciphering unit (FIG. 1, item 210) comprises: a first block having a first exclusive-OR operator for performing a logical exclusive-OR operation on the first sub-bit stream and the first encryption code KO.sub.1,1 (specification, page 3, lines 26-29), a first sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code KI.sub.1,1 (specification, page 3, lines 26-29), and a second exclusive-OR operator for generating a first signal by performing a logical exclusive-OR operation on the encrypted signal with the second sub-bit stream being delayed to provide time for the encryption (specification, page 4, lines 1-3); a second block having a third exclusive-OR operator for performing a logical exclusive-OR operation on the second sub-bit stream and the first encryption code KO.sub.1,2 (specification, page 4, lines 3-5), a second sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code KI.sub.1,2 (specification, page 4, lines 4-5), and a fourth exclusive-OR operator for generating the first operated ciphertext bit stream by performing a logical exclusive-OR operation on the encrypted signal and the first signal (specification, page 4, lines 7-8); and a third block having a fifth exclusive-OR operator for performing a logical exclusive-

OR operation on the first signal and the first encryption code KO.sub.1,3 (specification, page 4, lines 8-10), a third sub-cipher for encrypting the exclusive-OR-operated bit stream with the first encryption code KI.sub.1,3 (specification, page 4, line 10-11), and a sixth exclusive-OR operator for generating the second operated ciphertext bit stream by performing a logical exclusive-OR-operation on the encrypted signal and the first sub-bit stream delayed by time required for the encryption (specification, page 4, lines 11-14).

18. As to claim 10, AAPA discloses the encryption apparatus wherein the second ciphering unit (FIG.1, item 220) comprises: a fourth block having a seventh exclusive-OR operator for exclusive-OR-operating the first operated ciphertext bit stream with the encryption code (specification, page 3, lines 26-29), a fourth sub-cipher for encrypting the exclusive-OR-operated bit stream with the encryption code (specification, page 3, lines 29-30), and an eighth exclusive-OR operator for generating a second signal by performing a logical exclusive-OR-operation on the encrypted signal and the second operated ciphertext bit stream (specification, page 4, lines 2-3); a fifth block having a ninth exclusive-OR operator for exclusive-OR-operating the second operated ciphertext bit stream with the encryption code (specification, page 4, lines 3-5), a fifth sub-cipher for encrypting the exclusive-OR-operated bit stream with the encryption code (specification, page 4, line 5-6), and a tenth exclusive-OR operator for generating the third ciphertext bit stream by performing a logical exclusive-OR-operation on the encrypted signal (specification, page 4, line 5-8) and the second signal delayed by time required for the encryption (specification, page 4, line 8); and a sixth bock having an

eleventh exclusive-OR operator for performing a logical exclusive-OR operation on the second signal with the encryption code (specification, page 4, lines 8-10), a sixth sub-cipher for encrypting the exclusive-OR-operated bit stream with the encryption code (specification, page 4, lines 10-11), and a twelfth exclusive-OR operator for generating the fourth ciphertext bit stream by performing a logical exclusive-OR operation on the encrypted signal and the third ciphertext bit stream (specification, page 4, lines 11-14).

AAPA doesn't explicitly disclose the use of second-round encryption using predetermined second encryption codes KO.sub.2,1, KI.sub.2,1, KO.sub.2,2, KI.sub.2,2, KO.sub.2,3 and KI.sub.2,3. However, using second set of predetermined encryption code for second round encryption is standard in Kasumi encryption algorithm as taught by DKS (page 12, section 4.3, which describes KO.sub.i=KO.sub.i,1 || KO.sub.i,2 || KO.sub.i,3 and KI.sub.i= KI.sub.i,1 || KI.sub.i,2, || KI.sub.i,3, "i" reads on 2, see e.g., page 10, section 2.3, line 10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify AAPA by using second set of predetermined encryption code for second round encryption as taught by DKS in order to increase the confidentiality and integrity of the encrypted data. Furthermore, one would be motivated to do so to transmit data over the public network.

19. Claims 6, 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA in view DKS, in further view of Campbell, Jr. (Patent No.: 4,304,961), hereinafter "Campbell"

20. As to claim 6, AAPA discloses each of the encryptions includes first and second sub-encryptions (FIG. 3, items S91, S71 reads on first sub-encryption and items S92, S72 reads on second sub-encryption).

Neither AAPA nor DKS discloses the outputs from the first and second sub-encryptions are stored and simultaneously retrieved according to an external clock signal. However, Campbell discloses the outputs from the first and second sub-encryptions are stored and simultaneously retrieved according to an external clock signal (FIG. 1A, items 18, 20, 22, FIG. 2; column 5, lines 66-68 and column 6, lines 1-7 and 11-16).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify AAPA and DKS by storing the outputs from the first and second sub-encryptions and simultaneously retrieving according to an external clock signal as taught by Campbell in order to "provide and improved authenticator code generator for generating a unique authenticator code which is dependent on a key variable stored in the authenticator code generator and the text of a received message" (Campbell, column 3, lines 45-49).

21. As to claim 11, AAPA discloses each of the first to sixth sub-ciphers (FIG 1. items 210 and 220 each has three sub-ciphers, e.g., see FIG. 2A and FIG. 2B) includes first and second sub-ciphering units (FIG. 3, items S91, S71 reads on first sub-encryption and items S92, S72 reads on second sub-encryption).

Neither AAPA nor DKS discloses a register for storing the outputs of the first and second sub-ciphering units and simultaneously retrieve the outputs according to an external clock signal. However, Campbell discloses a register for storing the outputs of the first and second sub-ciphering units and simultaneously retrieves the outputs according to an external clock signal (FIG. 1A, items 18, 20, 22, FIG. 2; column 5, lines 66-68 and column 6, lines 1-7 and 11-16).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify AAPA and DKS by storing the outputs from the first and second sub-encryptions and simultaneously retrieving according to an external clock signal as taught by Campbell in order to "provide and improved authenticator code generator for generating a unique authenticator code which is dependent on a key variable stored in the authenticator code generator and the text of a received message" (Campbell, column 3, lines 45-49).

22. As to claim 12, AAPA discloses the encryption apparatus wherein each of the first and second sub-ciphering units divides a 16-bit input bit stream into a 9-bit stream and a 7-bit stream (specification, page 4, lines 22-24, FIG. 3), and generates a 9-bit ciphertext bit stream from the 9-bit stream using a third equation (specification, page 4,

lines 24-25), and a 7-bit ciphertext bit stream from the 7-bit stream using a fourth equation (specification, page 5, line 12), said third equation comprising y 0 = (x0x2) ⊕ x3 ⊕ (x2x5) ⊕ (x5x6) ⊕ (x0x7) ⊕ (x1x7) ⊕ (x2x7) ⊕ (x4x8) ⊕ (x5x8) ⊕ (x7x8) ' ⊕1 ' ; y 1 = x1 ⊕ (x0x1) ⊕ (x2x3) ⊕ (x0x4) ⊕ (x1x4) ⊕ (x0x5) ⊕ (x3x5) ⊕ x6 ⊕ (x1x7) ⊕ (x2x7) ⊕ (x5x8) ' ⊕1 ' ; y2 = x1 ⊕ (x0x3) ⊕ (x3x4) ⊕ (x0x5) ⊕ (x2x6) ⊕ (x3x6) ⊕ (x5x6) ⊕ (x4x7) ⊕ (x5x7) ⊕ (x6x7) ⊕ x8 ⊕ (x0x8) ' ⊕ 1 ' ; y3 = x0 ⊕ (x1x2) ⊕ (x0x3) ⊕ (x2x4) ⊕x5 ⊕ (x0x6) ⊕ (x1x6) ⊕ (x4x7) ⊕ (x0x8) ⊕ (x1x8) ⊕ (x7x8) ; y4 = (x0x1) ⊕ (x1x3) ⊕x4 ⊕ (x0x5) ⊕ (x3x6) ⊕ (x0x7) ⊕ (x6x7) ⊕ (x1x8) ⊕ (x2x8) ⊕ (x3x8) ; y5 = x2 ⊕ (x1x4) ⊕ (x4x5) ⊕ (x0x6) ⊕ (x1x6) ⊕ (x3x7) ⊕ (x4x7) ⊕ (x6x7) ⊕ (x5x8) ⊕ (x6x8) ⊕ (x7x8) ' ⊕1 ' ; y6 = x0 ⊕ (x2x3) ⊕ (x1x5) ⊕ (x2x5) ⊕ (x4x5) ⊕ (x3x6) ⊕ (x4x6) ⊕ (x5x6) ⊕x7 ⊕ (x1x8) ⊕ (x3x8) ⊕ (x5x8) ⊕ (x7x8) ; y7 = (x0x1) ⊕ (x0x2) ⊕ (x1x2) ⊕ x3 ⊕ (x0x3) ⊕ (x2x3) ⊕ (x4x5) ⊕ (x2x6) ⊕ (x3x6) ⊕ (x2x7) ⊕ (x5x7) ⊕x8 ' ⊕1 ' ; y8 = (x0x1) ⊕x2 ⊕ (x1x2) ⊕ (x3x4) ⊕ (x1x5) ⊕ (x2x5) ⊕ (x1x6) ⊕ (x4x6) ⊕ x7 ⊕ (x2x8) ⊕ (x3x8) (specification, page 5, line 1, equation 1);

Second equation comprises y 0 = (x1x3) ⊕ x4 ⊕ (x0x1x4) ⊕ x5 ⊕ (x2x5) ⊕ (x3x4x5) ⊕ x6 ⊕ (x0x6) ⊕ (x1x6) ⊕ (x3x6) ⊕ (x2x4x6) ⊕ (x1x5x6) ⊕ (x4x5x6) ; y 1 = (x0x1) ⊕ (x0x4) ⊕ (x2x4) ⊕ x5 ⊕ (x1x2x5) ⊕ (x0x3x5) ⊕ x6 ⊕ (x0x2x6) ⊕ (x3x6) ⊕ (x4x5x6) ' ⊕ 1 ' ; y2 = x0 ⊕ (x0x3) ⊕ (x2x3) ⊕ (x1x2x4) ⊕ (x0x3x4) ⊕ (x1x5) ⊕ (x0x2x5) ⊕ (x0x6) ⊕ (x0x1x6) ⊕ (x2x6) ⊕ (x4x6) ' ⊕ 1 ' ; y3 = x1 ⊕ (x0x1x2) ⊕ (x1x4) ⊕ (x3x4) ⊕ (x0x5) ⊕ (x0x1x5) ⊕ (x2x3x5) ⊕ (x1x4x5) ⊕ (x2x6

) ⊕ (x1x3x6) ; y4 = (x0x2) ⊕ x3 ⊕ (x1x3) ⊕ (x1x4) ⊕ (x0x1x4) ⊕ (x2x3x4) ⊕ (x0x5) ⊕ (x1x3x5) ⊕ (x0x4x5) ⊕ (x1x6) ⊕ (x3x6) ⊕ (x0x3x6) ⊕ (x5x6) ' ⊕1 ' ; y5 = x2 ⊕ (x0x2) ⊕ (x0x3) ⊕ (x1x2x3) ⊕ (x0x2x4) ⊕ (x0x5) ⊕ (x2x5) ⊕ (x4x5) ⊕ (x1x6) ⊕ (x1x2x6) ⊕ (x0x3x6) ⊕ (x3x4x6) ⊕ (x2x5x6) ' ⊕1 ' ; y6 = (x1x2) ⊕ (x0x1x3) ⊕ (x0x4) ⊕ (x1x5) ⊕ (x3x5) ⊕ x6 ⊕ (x0x1x6) ⊕ (x2x3x6) ⊕ (x1x4x6) ⊕ (x0x5x6) (specification, page 5, line 15, equation 2) ;

Conclusion

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892.

Matsui et. Al. (Pub. No.: US 2002/0131589) discloses to perform a plurality of sub-transformation in parallel to increase an processing speed of data transformation such as encryption.

Coppersmith et. Al. (Pub. No.: US 2003/0152219) discloses two non-liner permutations that operate on 64-bit blocks.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nabil M. El-Hady can be reached on 571 272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD
6D.

N. El-Hady

NABIL M. EL-HADY
SUPERVISORY PATENT EXAMINER